REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C	**7. Address**: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207

8. Title (Include Security Classification):
(U) Risks and Vulnerabilities of Network-Centric Forces: Insights from the Science of Complexity

9. Personal Authors:
Major Joseph H. Scherrer, USAF

10. Type of Report: FINAL	**11. Date of Report**: 03 February 2003

12. Page Count: 24 **12A Paper Advisor (if any):** Dr. Theodore Gatchel

13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: Network Centric Warfare, Operational Art, Critical Vulnerabilities, Command and Control, Complexity, Chaos, Information Technology, Operational Warfare, Transformation, Revolution in Military Affairs

15. Abstract: NCW relies heavily on complexity science concepts like complex adaptive systems, self-organization, and network effects to support its proponents' claims of decisive operational utility to the war fighter. While many commentators have critiqued NCW from the historical, national-strategic, and "human-centric" perspectives, little work has been done to analyze the science behind the concept. This despite the fact that leading scientists in the field of complexity science admit that much more work needs to be done before the science's relevance to organized human activities is definitively proven.

With the U.S. staking so much on network-centric capabilities, it is vital that the purported benefits of NCW be balanced by a frank assessment of its risks and vulnerabilities in anticipation of adversary challenges. For a combatant commander, the effects of an adversary intent on neutralizing or denying NCW's advantage will be immediately felt in the operational battlespace. As part of the operational planning process, a combatant commander's planning staff must identify the critical vulnerabilities associated with network-centric forces and formulate courses of action that mitigate risk and ensure operational protection of vital NCW capabilities.

The central thesis of this paper is that the use of network-centric forces introduces risks and vulnerabilities that affect a combatant commander's ability to conduct operational warfare. An analysis is presented that illustrates potential risks and vulnerabilities of NCW, and recommendations are made that might help a combatant commander and a joint planning staff cope with them.

16. Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**

17. Abstract Security Classification: UNCLASSIFIED

18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. Telephone: 841-3556	**20. Office Symbol:** C

Security Classification of This Page Unclassified

(Unclassified Paper)

NAVAL WAR COLLEGE
Newport, R.I.

RISKS AND VULNERABILITIES OF NETWORK-CENTRIC FORCES:

INSIGHTS FROM THE SCIENCE OF COMPLEXITY

by

Joseph H. Scherrer

Major, United States Air Force

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: //signed//--jhs-3 Feb 03
JOSEPH H. SCHERRER, Major, USAF

3 February 2003

INTRODUCTION

We must use all types, forms, and methods of force, and especially make more use of nonlinear warfare and many types of information warfare methods which combine native and Western elements to use our strengths in order to attack the enemy's weaknesses, avoid being reactive, and strive for being active. In this way, it will be entirely possible for China to achieve comprehensive victory over the enemy even under the conditions of inferiority in information technology.

General Wang Pufeng, Chinese Red Army

Network-centric warfare (NCW) increasingly is becoming a new orthodoxy—a set of beliefs that cannot seriously be challenged. Its disadvantages or critical vulnerabilities are not publicly discussed or are grudgingly admitted…The enemy rarely is mentioned, and he seems to be incapable of frustrating our plans and actions.

Dr. Milan Vego

China is not the only potential adversary thinking deeply about how to combat the U.S. military's information technology advantage. Other rivals will also seek to challenge, match, and even surpass this advantage. These efforts should not surprise us: the history of war is in large part the story of combatants using technology to achieve a competitive edge.[1] The inevitability of a challenge to NCW gives rise to compelling questions: what are the risks and vulnerabilities of NCW and how might we cope with them?

Unfortunately, as Vego implies, the momentum created by NCW appears to be shunting aside any meaningful consideration of these questions.[2] For example, NCW relies heavily on complexity science concepts like complex adaptive systems, self-organization, and network effects to support its proponents' claims of decisive operational utility to the war fighter.[3] While many commentators have critiqued NCW from the historical, national-strategic, and "human-centric" perspectives, little work has been done to analyze the science behind the concept.[4] This despite the fact that leading

scientists in the field of complexity science admit that much more work needs to be done before the science's relevance to organized human activities is definitively proven.[5]

With the U.S. staking so much on network-centric capabilities, it is vital that the purported benefits of NCW be balanced by a frank assessment of its risks and vulnerabilities in anticipation of adversary challenges. For a combatant commander, the effects of an adversary intent on neutralizing or denying NCW's advantage will be immediately felt in the operational battlespace. As part of the operational planning process, a combatant commander's planning staff must identify the critical vulnerabilities associated with network-centric forces and formulate courses of action that mitigate risk and ensure operational protection of vital NCW capabilities.

The central thesis of this paper is that the use of network-centric forces introduces risks and vulnerabilities that affect a combatant commander's ability to conduct operational warfare. Analysis reveals three categories of risks and vulnerabilities. First, the complex adaptive behavior of network-centric forces are unpredictable and sensitive to degradation or disruption. Second, self-organized synchronization of network-centric operations is impossible. Third, network effects give rise to unavoidable friction in decision cycles and opens the network to new forms of attack.

To further explain these issues, an overview of complexity science is presented along with definitions of complex adaptive systems, self-organization, and network effects. Next, NCW and its relation to complexity science are described. Then, the link between NCW and complexity science is examined to determine what risks and vulnerabilities might arise from the use of network-centric forces. Following an

alternative view of the analysis, recommendations are made that may help a combatant commander and joint planning staffs cope with NCW's risks and vulnerabilities.

COMPLEXITY SCIENCE

Complexity science holds that evolution and survival occur most effectively when large numbers of entities mutually interact.[6] A popular example of complexity at work is a flock of birds. Operating under simple rules, birds orient on their immediate neighbors to form a V-shaped, self-organized, cooperative system. Complexity science seeks to discover the general rules that underlie the behavior of such systems through observation, experimentation, analysis, and computer modeling.[7]

In addition to animal grouping behavior, attempts have been made to apply complexity science to the behavior of molecules, the actions of nation states, the balance of nature, and business competition. In the business arena, a large literature and practice have emerged to help businesses apply the concepts of complexity science and improve their ability to adapt, evolve, and compete in the marketplace.[8] This business phenomenon helps to explain how NCW incorporated concepts from complexity science like complex adaptive systems, self-organization, and network effects. These concepts are now examined in more detail.

Complex Adaptive Systems

Complex adaptive systems, such as termite colonies and the immune system, consist of a large number of components mutually interacting in a dynamic manner.[9] Complex adaptive systems are not directed by a central control mechanism. Rather, coherent patterns of behavior emerge from competition and cooperation among the

agents in the system. Importantly, each individual component is unaware of the behavior of the complex adaptive system as a whole.[10]

The components of a complex adaptive system continually adapt by changing their internal behavioral rules as the environment and their experience of that environment evolves over time.[11] As a result, complex adaptive systems remain in constant states of flux and are both resilient and potentially sensitive to changes in environmental conditions.[a] Sensitivity means that even small inputs, disturbances, or feedback in the system can result in very large changes in behavior. Moreover, since the exact state of the environment and the exact behavior of other agents can never be known at a global level due to the myriad of components and interactions, it is only possible to optimize individual behavior rather than overall complex adaptive system behavior. As a result, the behavior of complex adaptive systems is generally unpredictable. The aggregate result of these characteristics is that complex adaptive systems operate at the "edge of chaos" between states of stable equilibrium and ultimate disorder or chaos. Operating at the edge of chaos requires great amounts of energy, but some researchers believe that such systems are better able to formulate multiple response options to deal with a given range of environmental conditions.

Self-Organization

Self-organization refers to the overall global behavior that arises in complex adaptive systems. This behavior emerges due to the collective interactions of the system's component parts as these parts react and adapt to their environment.[12] In a self-organized complex adaptive system, there is no top-down direction of components.

[a] Discussion summarized from Eoyang and Berkas, "Evaluation in a Complex Adaptive System," In *Managing Complexity in Organizations*, eds. Lissak and Guns, (Westport: Quorum Books, 1998), 4-8.

Rather, parts act locally (tactically) on local information and overall order emerges without the need for hierarchical control. Importantly, global behavior cannot be predicted by examining the properties and interactions of the system's components.

Network Effects

Network effects occur in businesses that operate as networked, self-organized complex adaptive systems. These businesses are better able to seize, grow, and hold market share at extremely low cost as more consumers adopt their products.[13] Network effects provide positive feedback leading to increasing returns to scale, monopoly like profits, and "lock-out" of competition. Two key components of network effects are relevant to NCW: Metcalfe's law and power law behavior.

Metcalfe's Law states that the value of a network grows with the square of the number of participants.[14] In other words, each additional member of a network adds an incremental amount of value to every other member, thus increasing the aggregate value of the network. Given the choice of joining a large existing network with many users or a smaller one with few users, new users will decide that the bigger one is far more valuable, often resulting in explosive growth once a network establishes dominance.

When combined with actual network growth behavior like that found in the Internet, Metcalfe's law is often found alongside network power law behavior. Characteristic of certain types of complex adaptive systems, power law behavior means that as a network grows, some nodes become more connected than others.[b] In this "rich get richer" situation, very few hubs connect most users, medium sized hubs connect intermediate-sized groups of users, and many small hubs connect small clusters of users.

[b] The explanation of network-based power laws is summarized from Barabasi in *Linked: The New Science of Networks*, (Cambridge: Perseus Publishing, 2002).

As the network grows, the ratio of very connected hubs, medium-sized hubs, and small hubs remains constant.

NETWORK-CENTRIC WARFARE

Advocates of NCW define it as, "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization."[15] NCW proponents also assert that NCW applies to all levels of war: tactical, operational and strategic. According to Cebrowski and Gartska, "NCW seeks to leverage complexity through networked situational awareness, increased speed of command resulting in OODA loop [observe, orient, decide, act] dominance and adversary lock-out."[16] Advocates of NCW claim that the NCW assists commanders and personnel at the "cognitive" level of war meaning that information and how it is processed and interpreted in the minds of the combatants is just as important—if not more important—than the information itself.[17] Quicker, more accurate assessments lead to decisions that heavily influence the outcome of battle.

NCW and Complex Adaptive Systems

Cebrowski and Gartska use observations from the business arena to argue that NCW is in part the military response to a broad societal shift from viewing actors like businesses and nations as independent to viewing them as part of continuously adapting ecosystems.[18] This view emphasizes the close linkage and interdependence of actors in business ecosystems. The military mirrors this interdependence through the linkages and interactions among units and the operating environment.[19] This complex organization

relies on doctrine, training, and a chain of command that enables units and personnel to operate as complex adaptive systems and achieve tightly coupled, high-impact effects.[20]

NCW and Self-Organization

NCW advocates adapt complexity science's definition of self-organization and add the term "synchronization" from operational art to create the concept of self-synchronization. Self-synchronization is the ability of a well-informed force to organize and synchronize warfare activities from the bottom-up.[21] Self-synchronization requires two or more robustly networked entities, shared awareness, a rule set, and a value-adding interaction.[c] The combination of a rule set specifying the desired outcomes for a variety of operational situations, shared awareness, and communications enables the entities to operate in the absence of traditional hierarchical mechanisms for command and control. Self-synchronized forces are decentralized, with decision-making pushed down to the lowest levels, and decisions guided by training, understanding of commander's intent, and shared situational awareness.

NCW and Network Effects

NCW advocates cite Metcalfe's law to explain the potential value of interconnecting the battlespace into a massive network of users, sensors, and shooters. For NCW, high quality information exchange between nodes characterizes the value of this interconnected network. Speeded acquisition of actionable information leads to a superior information position and better situational awareness relative to an adversary. Information superiority is achieved when a competitive advantage is derived from the

[c] The self-synchronization and network effects discussions rely on Alberts et al, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 103-108 and 175-176.

ability to exploit a superior information position. Without a network in NCW, the likelihood of achieving information superiority is greatly reduced.

ANALYSIS

Risks and Vulnerabilities of Complex Adaptive Behavior

If network-centric forces are truly complex adaptive systems, then they may indeed prove robust, adaptable, and flexible across a wide range of situations—appealing characteristics to be sure. However, complexity science shows that these same network-centric systems are subject to unpredictable and potentially large changes in behavior. These changes could arise from seemingly small inputs to the network-centric system and make their behavior as uncertain as predicting the weather.[22] Under such circumstances, complex adaptive network-centric forces operating at the edge of chaos could become more sensitive to disruption. An adversary with an understanding of complexity science could systematically cut off the system's ties to the environment, depriving it of the energy needed to remain at the edge of chaos and driving it to lower levels of equilibrium and capability. For example, Allied attacks on Axis shipping to North Africa during World War II constrained Rommel's ability to fight his armored forces and were a key factor in his defeat.[23] Though arguably still tactically superior to the Allies, the logistics crisis drove Rommel's "complex adaptive" forces to lower levels of capability that restricted his ability to fight at the operational level.

At the other end of the complexity spectrum, an adversary could deliberately induce disturbances designed to push the network-centric system into chaos. Overloading sensor and shooter network grids in combination with the employment of weapons of mass destruction and continuous conventional attacks is a way to drive

network-centric forces into chaos and disintegrate warfighting capability. Unable to operate, a combatant commander's forces become vulnerable to defeat in detail or are forced to adopt different, less efficient, and less effective modes of warfare.[24]

Applying the scientific principles of complex adaptive systems to NCW indicates that the reactions of network-centric forces are unpredictable and sensitive to degradation or disruption. Lower levels of equilibrium or chaos neutralize NCW-enabled agility, adaptability, and speed of command, causing the combatant commander to fight in a different manner or on terms dictated by the adversary. Planners must balance the benefits of complex adaptive forces against these risks.

Risks and Vulnerabilities of Self-Organized Synchronization

Self-synchronization is arguably the operational core of NCW, and seems intuitively workable. However, upon closer inspection, self-synchronization might make operational synchronization impossible. According to Vego, operational synchronization is the deliberate arrangement of actions in space, time, and purpose to deliver effects and generate the maximum relative combat or non-combat power at a decisive place and time during a major operation or campaign.[25] At a fundamental level, combining the concepts of self-organization with synchronization yields a construct at odds with itself.

Operational synchronization is purposeful, planned, and centrally controlled. In contrast, NCW-based self-synchronization is ad-hoc, real-time, unplanned, and—according to the science of self-organization—uncontrolled and unmanaged. The German offensive at the Somme in 1918 illustrates the hazards of self-synchronization at the operational level. The German counter-attack was guided by the prime consideration of pressing the initiative using independently operating forces. These forces recaptured

in four days territory that the British had fought over for four months.[26] Despite a degree of self-synchronization at the tactical level, the Germans were unable to exploit the breakthrough. This failure can be partly attributed to the breakdowns in headquarters communications and the German troops themselves, who, fatigued after continuous combat, began to loot British stores rather than pressing the attack.[27]

An obvious challenge arises for a combatant commander charged with the responsibility of synchronizing inherently unsynchronizable network-centric forces. As the German example demonstrates, it is unclear how tactical forces would be able to retain the operational outlook to routinely formulate operational level courses of action, account for adversary intentions, focus combat power across units and services, and consistently achieve operational effects—all while remaining engaged tactically.[28] As a result, joint planners and decision-makers are faced with an almost intractable problem when working to synchronize forces at the operational level.

Risks and Vulnerabilities of Network Effects

If Metcalfe's Law is taken at face value, it appears that the bigger the network supporting NCW, the better. However, as the size of a network grows, a point is reached where the addition of new users or information capabilities like databases, web sites, and sensors do not add value but may actually reduce it.[29] Larger and larger numbers of users and information capabilities adversely affects a user's ability to communicate over the network due to saturation and noise. The sheer volume of information on a large network leads to problems in linking up with other users and searching for, correlating, maintaining, and interpreting information.[30] Recent operations in Kosovo show how massive quantities of video and imagery can strain the ability of a network to supply the

right information, at the right place, at the right time.[31] In addition, the character of information itself and the interpretation of that information may actually contribute to friction in war.[32] It is conceivable that highly networked forces will increase this friction even further, degrading a combatant commander's capacity to achieve conditions favoring speed of command and decision superiority.

It is also important for a combatant commander to be aware of the potential vulnerabilities introduced by power law networks. While these networks have been shown to be highly resilient to random node failures, this situation changes if the most connected hubs are systematically attacked.[d] In a network-centric complex adaptive system, the destruction of just a few large hubs could cause the network to fail. U.S. targeting methodologies focus on just such effects as illustrated by attacks on Iraqi command and control nodes in the Gulf War and the Serbian power grid during the Kosovo conflict. In addition, power law networks are vulnerable to "cascade" attacks. This type of attack targets the automatic re-routing capability of a network. Carefully planned attacks can lead to a cascade of overload failures, which can in turn cause the entire or a substantial part of the network to collapse. The very diversity of NCW networks makes them particularly vulnerable to attacks in that disabling a single key node triggers a large-scale cascade outage—an example of an asymmetry at work. Hub and cascade attacks against an NCW-enabled force paralyze command processes and degrade a Joint Force Commander's ability to operate.

[d] Information on hub and cascade attacks is sourced from Barabasi, *Linked: The New Science of Networks*, 111-122.

COUNTER PERSPECTIVE

Some would argue that despite any risks and vulnerabilities associated with NCW's link to complexity science, the intuitive benefits the science offers is enough for the U.S. to proceed to alter its technology, training, and organizations to accommodate NCW's perceived and emerging validity.[33] If not, potential adversaries may leap ahead in their ability to operate network-centrically and exploit its potential benefits. Failure to transform may result in the U.S. finding itself in the same position as Britain and France in 1939. Furthermore, NCW supporters believe there is sufficient empirical evidence from history, business, and tactical-level combat to justify the move to NCW.[34] Others might argue that had the Germans in 1918, Rommel in 1943, or even U.S. forces in Somalia been fully netted, the outcomes of these campaigns and operations might have been very different. Even a small relative information advantage offered by netted forces is sufficient reason to move forward to NCW. In addition, as the success of information age businesses show, adoption of NCW capabilities is necessary for the U.S. military to gain and retain a "first-mover" advantage.[35]

NCW advocates might also point out that they have tempered their claims along the way to account for the uncertainties that underlie NCW. Several "Myths of NCW" have been put forth that state, "Sorting out fact from fancy will be among the community's principal task as we grapple with how to apply network-centric concepts to military operations."[36] Others cite the need for NCW to mature through research, field experimentation, war gaming, and exercises.[37] It is reasonable to assume that a treatment of risks and vulnerabilities such as those touched on in this paper would be welcomed by the NCW community as an opportunity to improve the concept.

RECOMMENDATIONS

The proponents of NCW are correct that the U.S. has little choice but to continue to leverage technology to improve its warfighting capacity. However, a willingness to revisit and revise NCW in light of the findings of this paper is essential to improving its relevance to operational warfare and reducing its risk. Based on the analysis, the way in which NCW uses complexity science is flawed. Though the findings do not entirely negate the potential of NCW, they are of sufficient gravity to suggest that a more tempered and cautious approach to the concept is needed. Given the current overwhelming U.S. military-technological advantage—an advantage that is not likely to be surpassed anytime soon—breathing room is available to more thoroughly vet the concept. To use this time wisely, several approaches are possible to ensure NCW remains a viable and promising warfighting vision.

First, budget for and fund a comprehensive science and technology research program that furthers the understanding and application of the links between the science of complexity and warfare. The research program must undertake a critical reexamination of the theoretical basis of NCW. As shown in the analysis, NCW's use of complex adaptive systems and self-synchronization does not entirely incorporate the full scientific meanings of the terms. If the science of complexity truly applies to warfare, then the rules and characteristics that accompany them must be accepted in full: fundamental truths of nature cannot be conveniently ignored. A rigorous reformulation of NCW that fully accounts for the science of complexity will yield a concept with increased validity and applicability to the military practitioner.

In addition, given the fact that the U.S. military spends enormous amounts of money and time to ensure that its forces produce reasonably consistent results and behavior in arduous environments, building a force that has the capacity for inherently unpredictable behavior—including a network-centric force—is not prudent. Research must be undertaken before such forces are fielded to discover where the thresholds of uncertainty lie and in what circumstances unpredictability appears. Investigation into self-organizing behavior and how it might be adapted to allow a degree of control in combat situations is also needed. Similarly, a rigorous investigation of the structure of military networks to discover the scope to which they follow power law behavior and the extent to which they are vulnerable to hub and cascade attacks is strongly recommended. This portion of the research program must focus on engineering methodologies that remove or reduce vulnerabilities as well as the development of operational protection measures. The methodologies and measures—whether technological, organizational, or procedural—should better enable joint forces to plan for, engineer, and defend against adversary command and control warfare. Additionally, the research must suggest management strategies to reduce the operational risk of network-centric forces. Finally, a systematic program of experimentation, "red teaming", and testing must occur before network-centric capabilities are introduced to the joint force.

There is a danger that the momentum behind NCW eclipses the institutional will to slow implementation of NCW and engage in more systematic research into the concept. Given NCW's potential to affect operational warfare, a combatant commander needs concrete recommendations on how to handle its risks and vulnerabilities. While a complete examination of the implications of NCW on operational warfare is outside the

scope of this paper, several recommendations in the areas of training, operational planning, operational command and control, and operational protection can be made.

As the NCW concept finds its way more and more into the operational environment, decision-makers, joint force planners, and battle managers must be required to undergo a block of training that familiarizes them with the possible benefits and hazards of NCW. Particular attention must be given to the impacts on operational planning, operational command and control, and operational protection and practical techniques that maximize NCW's benefits and minimize its vulnerabilities.

With regard to operational planning, a joint planning staff must ensure that operational synchronization is maintained throughout a major operation or campaign while also accounting for the capacity of NCW-enabled self-synchronization during execution. During the planning process, forces with the capacity for self-synchronization must be provisioned with guidance and rules of engagement that focus this capacity in order to shape their actions so that they are in accordance with the strategic and operational objectives. However, given the risk that self-synchronization introduces, use of these forces must be limited to tightly focused tactical actions until the full operational-level ramifications of NCW are worked out.

The use of any type of network-centric operations will require a combatant commander to carefully consider the function of operational command and control. Because NCW relies heavily on decentralized control and execution (control is not possible if NCW forces are true complex adaptive systems), networked command structures must be augmented with clear, unambiguous business rules that specify the extent to which higher-echelon command approval is needed and horizontal coordination

is authorized. For particular types and levels of forces, especially network centric capable forces, the information flows that create situational awareness must be tailored and structured to prevent information overload while also ensuring that the right elements of information are provided. In addition, a distinction must be made between the information needed at the operational and tactical levels. For instance, U.S. Air Force air defense forces employ strict procedures to control and distribute information that clearly separate operational and tactical command echelons.[38] These procedures help to ensure that fires are coordinated, force is not wasted, and fratricide is avoided.[39] Similar safeguards must be crafted to ensure that network-centric forces contribute fully to the tactical level fight while at the same time ensuring the accomplishment of and limiting the risk to operational objectives.

Operational protection of the infrastructure that supports NCW becomes a prime concern of a combatant commander. Given the vulnerabilities inherent in networks that exhibit power law behavior, information assurance mechanisms and countermeasures must be put in place to protect them. While scientific research will aid joint force network planners and engineers in accomplishing this task, recognition that such vulnerabilities exist allows for more prudent infrastructure design and management. As part of the design process, netted "hotspots" such as hubs and key command and control nodes must be identified. These hotspots must be engineered for increased survivability and redundancy to include high levels of parts sparing as well as circuit path and mode diversity. In addition, careful network design will allow the number of hubs to be reduced or normalized to present a more random distribution that in turn would increase network survivability. Preemptive countermeasures such as "red team" modeling will aid

in uncovering network vulnerabilities and anticipating and protecting against adversary methods of hub and cascade attack.

CONCLUSION

> When you can measure what you are talking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind: it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science.
>
> Lord Kelvin

It is almost axiomatic that the U.S. must continue to improve the efficiency and effectiveness of its warfighting capability. What is harder to argue is that changes be made headlong without due consideration of the risks and vulnerabilities of operating the military as a self-organized complex adaptive system and to what extent these risks and vulnerabilities will affect operational warfare. This paper represents a first step in this direction. As the analysis showed, when viewed through the lens of complexity science, the potential benefits of NCW are more than balanced by its potential drawbacks. Both must be considered in the employment of network-centric forces.

Complexity science analogies like those used in NCW, though insightful, are not proof that the science is applicable. It remains to be demonstrated convincingly that the kinds of dynamic effects identified by applications of complexity science automatically translate into the kinds of dynamics seen in warfare. Much more research must be done as the U.S. moves down the road to an NCW-enabled force. At present, it is more advisable to view the link between complexity science and NCW in terms of the conceptual insight it offers rather than its decisiveness in explaining reality. When viewed in this way, NCW's greatest benefit is in helping to shape new visions and build

alternative models of warfare. Any other approach opens a combatant commander to risks and vulnerabilities that might otherwise be avoided.

NOTES

[1] Martin Van Crevald, *Technology in War* (New York: The Free Press, 1991), 1-6. Van Crevald explains in a compelling fashion how technology has been a part of the human experience of war since time immemorial.

[2] A case in point might be drawn from the controversy surrounding the 2002 Millenium Challenge war game run by U.S. Joint Forces Command. This $250 million effort was "almost entirely scripted to ensure a Blue win" according to Red Team Commander retired Marine Lt. Gen. Paul Van Riper who quit the post halfway through the game. From an article by Mackubin Owens, *Wall Street Journal*, 29 August 2002, Opinion Page.

[3] David S. Alberts et al, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition, Revised (Washington DC: CCRP Publication Series, 1999), 88.

[4] See T.X. Hammes, "War Isn't a Rational Business," *U.S. Naval Institute Proceedings* (July 1998): 22-25 and Alan D. Zimm, "Human-Centric Warfare," *U.S. Naval Institute Proceedings* (May 1999): 28-31 for arguments supporting the need for human centered approaches to NCW. Also, Richard J. Harknett and the JCISS Study Group, "The Risks of a Networked Military," *Orbis* (Winter 2000): 127-143 provide a national strategic argument for a cautious approach to NCW.

[5] Alvin M. Saperstein, "Complexity, Chaos, and National Security Policy: Metaphors or Tools?" in *Complexity, Global Politics, and National Security*, eds. David S. Alberts and Thomas J. Czerwinski (Washington DC: CCRP Publication Series, 1999), 125. Saperstein, an international relations professor, asserts that, "When all is said and done, on a strategic level, the most useful aspect of the chaos and complexity metaphors is to remind us and help us to avoid falling into chaos." Also, Stuart A. Kauffman, *At Home in the Universe* (New York: Oxford University Press, 1995). Kauffman's entire book, though optimistic about complexity science's application to human affairs, is essentially a "what-if" presentation on the application of molecular and biological complexity science to larger phenomena such as economies and international relations.

[6] M. Mitchell Waldrop, *Complexity: The Emerging Science at the Edge of Order and Chaos*, (New York: Touchstone, 1987), 11-12.

[7] Ibid, 9-12.

[8] Peter M. Senge, an organizational learning specialist, is arguably one of first to integrate complexity theory into a business context. Scores of others, including prominent complexity researchers like Stuart Kauffman, have jumped on the bandwagon. See Senge's *The Fifth Discipline: The Art and Practice of the Learning Organization* (New York: Doubleday, 1990), 6-7 for an indication of his approach to complexity and business.

[9] Andrew Ilachinski, *Land Warfare and Complexity, Part I: Mathematical Background and Technical Sourcebook* (Washington DC: Center for Naval Analyses, 1996), 97. Ilachinski conducted a study of agent-based modeling for the United States Marine Corps. The study showed how the sciences of complexity and chaos could be applied to land and small unit warfare modeling and simulation. His three volume work is one of the most extensive treatments on the subject to date.

[10] Scott Camazine et al, *Self-Organization in Biological Systems* (Princeton: Princeton University Press, 2001), 8.

[11] Ibid, 97.

[12] Ibid, 7-11.

[13] W. Brian Arthur, "Complexity and the Economy," *Science (2* April 1999): 107-109. Also, S. J. Liebowitz and Stephen Margolis, "Path Dependence, Lock-In, and History," *Journal of Law, Economics and Organization* (November 1995): 205-226.

[14] Paul Metcalfe, "Metcalfe's Law: A Network Becomes More Valuable as it Reaches More Users," *Infoworld* (2 October 1995): 53. Metcalfe invented the Ethernet local area network protocol that underpins all network communications. He later went on to found the 3Com Corporation. The mathematics behind Metcalfe's law is based on graph theory and is a measure of the number of possible connections in a network when every node is connected to every other node. Metcalfe took this mathematical principle and linked it to network value and the ability of many people to interact with many other people.

[15] Alberts et al, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 88.

[16] Arthur Cebrowski and John J. Gartska, "Network Centric Warfare; Its Origin and Future," *U.S. Naval Institute Proceedings* (January 1998): 32. Cebrowski and Gartska unabashedly assert that NCW "will prove to be the most important RMA in the past 200 years." Also, John J. Gartska, "Network-Centric Warfare: An Overview of Emerging Theory," *Phalanx* (December 2000): 2.

[17] Edward A. Smith, Jr., "Network-Centric Warfare: What's the Point?" *Naval War College Review* (Winter 2001): 64. Smith explicitly links NCW to the emerging strategic concept called "effects-based operations". NCW is advertised to be the prime enabler of such operations by virtue of its ability to "get inside an adversary's OODA loop."

[18] Cebrowski and Gartska, "Network Centric Warfare: Its Origin and Future," 32-33. Cebrowski and Gartska translate lessons from "information age" business to assert that leveraging chaos and complexity through bottom-up organization provides the best way for military forces to achieve success.

[19] Ibid, 29-31.

[20] Arthur K. Cebrowski, "Network Centric Warfare: An Emerging Military Response to the Information Age," Presentation at the 1999 Command and Control Research and Technology Symposium, Naval War College, 29 June 1999, 2-4.

[21] Cebrowski and Gartska, "Network Centric Warfare; Its Origin and Future," 32-33.

[22] James Gleick, *Chaos, Making a New Science*, (New York: Penguin Books, 1987), 15-21. Edward Lorenz "discovered" chaos science while attempting to model and predict weather patterns. He found that small changes in initial weather equation variables resulted in dramatic changes in overall weather behavior and that such behavior was unpredictable. This is often called the "butterfly effect."

[23] Alan J. Levine, *The War Against Rommel's Supply Lines, 1942-1943* (Westport, CT: Praeger Publishers, 1999), viii, 145, 181. Levine's study details Allied interdiction operations and shows how loss of logistics resupply hampered Axis operations in North Africa. Though other factors certainly contributed to Rommel's defeat such as Hitler's intransigent strategic shortsightedness and Allied materiel superiority, lack of supplies severely limited Rommel's ability to operate.

[24] See Mao Tse Tung, *On Guerrilla Warfare*, trans. Samuel B. Griffith (Urbana: University of Illinois Press, 1961) and Vo Nguyen Giap and Van Tien Dung, *How We Won the War* (Philadelphia: Recon Publishing, 1976) for a discussion of how to operate at lower levels of equilibrium against a technologically superior adversary. It is interesting to think how well the U.S. military would be able to adjust to such an adversary.

[25] Milan N. Vego, *Operational Warfare* (Newport: Naval War College Press), 545.

[26] Martin Van Crevald, *Command in War* (New York: The Free Press), 168. Also, Timothy L. Lupfer, *The Dynamics of Doctrine: The Changes in German Tactical Doctrine During the First World War*, Leavenworth Papers (Fort Leavenworth: Combat Studies Institute, U.S. Army Command and General Staff College, 1981): 53.

[27] Ibid, 181.

[28] Thomas P. Barnett, "The Seven Deadly Sins of Network Centric Warfare," *U.S. Naval Institute Proceedings* (January 1999): 38.

[29] Andrew McAfee and Francois-Xavier Oliveau, "Confronting the Limits of Networks," *MIT Sloan Management Review* (Summer 2002): 85-87. McAfee and Oliveau discuss how the value of a network does not infinitely increase. As a network grows, issues of saturation, cacophony, contamination, clustering, and search costs combine to reduce its value. See also Paul Windrum and G.M. Peter Swann, *Networks, Noise, and Web Navigation: Sustaining Metcalfe's Law through Innovation*, MERIT Paper 009, (Maastricht: Maastrict Economic Research Institute on Innovation and Technology, 1999): 1-22. Both articles suggest ways to mitigate the impact of limits to Metacalfe's Law.

[30] Tor Norretranders, *The User Illusion* (New York: Penguin Books, 1998), 91-100 and Lawrence Shattuck, "Communicating Intent and Imparting Presence," *Military Review* (March-April 2000): 66-72. These two diverse pieces both address the subject of information interpretation and the subjectivity of meaning.

[31] James O. Ellis, "A View from the Top," Unpublished briefing slides, Headquarters Allied Forces Southern Europe, 4 July 1999.

See also Timothy T. Thomas, "Kosovo and the Current Myth of Information Superiority," *Parameters* (Spring 2000): 13-29. Commander of allied air forces during NATO Operation ALLIED FORCE, Adm Ellis's conclusion was that "information superiority overload can actually hurt mission performance." Col Thomas reinforces Adm Ellis's conclusion and shows how Serbian forces were able to deceive allied commanders using camoflage and decoys.

[32] See Barry D. Watts, *Clausewitzian Friction and Future War*, McNair Paper 52 *(*Washington DC: Institute for National Security Studies, National Defense University Press, 1996): 75-78. Watts differentiates between explicit knowledge ("meaningful information that is available for entry into databases and information systems") and tacit knowledge ("human capabilities to know or sense more than can be explicitly told or specified"). Well-formed and well-distributed tacit knowledge can give a military force great advantages over an adversary while the opposite can invite disaster. Watts suggests that variance in tacit knowledge and its inherent distributed nature is a permanent source of friction in war. Though it does seem reasonable that NCW might facilitate the gathering and distribution of explicit knowledge across a wide range of users, little is said about the role of tacit knowledge or how NCW might help marshal this vital resource across a network or reduce the friction inherent in it.

Also, Carol McCann and Ross Pigeau, *The Human in Command: Exploring the Modern Military Experience* (New York: Kluwer Academic/Plenum Publishers, 2000), 163-184. McCann and Pigeau address explicit and implicit commander's intent in terms of human-centered command and control. Explicit intent is publicly communicated while implicit intent is unvocalized or even unvocalizable. They argue that communicating implicit intent through personal, military, and cultural expectations is crucial to properly communicating the full meaning of commander's intent. Relying as it does on commander's intent to self-synchronize forces, NCW does not explain how it will improve this process or ensure "correct" interpretation of commander's intent across an NCW-enabled force. Misinterpreting commander's intent in a network-centric force could magnify the difficulty of self-synchronizing the force to meet that intent.

[33] William Owens, "An Emerging System of Systems," *U.S. Naval Institute Proceedings* (May 1995): 39. Owens makes the case that technological change in the form of a "system of systems" is a mandatory requirement for the success of U.S. military forces in the 21st century.

[34] Cebrowski and Gartska argue that information age changes are inevitable and that sufficient evidence exists from business and certain aspects of military operations to justify the move to NCW. See "Network Centric Warfare: An Emerging Response to the Information Age."

[35] Alberts et al, *Understanding Information Age Warfare* (Washington DC: C4ISR Cooperative Research Program, 2001), 294-299.

[36] Alberts et al, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 5-13.

[37] Cebrowski, "Network Centric Warfare: An Emerging Military Response to the Information Age,": 1.

[38] LtGen Leslie Kenne, "Tightening the Noose: Separating the Control of Information from the Command, Control of Forces," *Intelligence, Surveillance, and Reconnaissance Journal* (January-February 2003): 10.

[39] Ibid, 10.

BIBLIOGRAPHY

Alberts, David S., John J. Gartska, Richard E. Hayes, and David A. Signori. *Understanding Information Age Warfare*. Washington, DC: C4ISR Cooperative Research Program Publication Series, 2001.

Alberts, David S., John J. Gartska, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised). Washington, DC: C4ISR Cooperative Research Program Publication Series, 1999.

Arthur, Brian W. "Complexity and the Economy." *Science* (2 April 1999): 107-109.

Barabasi, Albert-Lazlo. *Linked: The New Science of Networks*. Cambridge, MA: Perseus Books, 2002.

Barnett, Thomas P. "The Seven Deadly Sins of Network Centric Warfare." *U.S. Naval Institute Proceedings* (January 1999): 36-39.

Bartlett, John, comp. *Familiar Quotations: A Collection of Passages, Phrases and Proverbs Traced to Their Sources in Ancient and Modern Literature*, 15th Edition. Revised and enlarged by Emily Morison Beck. Boston: Little, Brown and Company, 1980.

Camazine, Scott, Jean-Louis Deneubourg, Nigel R. Franks, James Sneyd, Guy Theraulaz, and Eric Bonabeau. *Self-Organization in Biological Systems*. Princeton, NJ: Princeton University Press, 2001.

Cebrowski, Arthur K. and John J. Gartska. "Network-Centric Warfare: Its Origin and Future." *U.S. Naval Institute Proceedings* (January 1998): 28-35.

Ellis, James O. "A View from the Top." Unpublished Briefing Slides, Headquarters, Allied Forces Southern Command, Naples, IT: 4 July 1999.

Eoyang, Glenda H. and Thomas H. Berkas. "Evaluation in a Complex Adaptive System." In *Managing Complexity in Organizations*, edited by M. Lissack and H. Gunz, 313-335. Westport, CT: Quorum Books, 1999.

Gartska, John J. "Network Centric Warfare: An Overview of Emerging Theory." *Phalanx* (December 2000): 1-33.

Giap, Vo Nguyen and Van Tien Dung. *How We Won the War*. Philadelphia: Recon Publishing, 1976.

Hammes, T. X. "War Isn't a Rational Business." *U.S. Naval Institute Proceedings* (July 1998): 22-25.

Harknett, Richard J. and the JCISS Study Group. "The Risks of a Networked Military." *Orbis* (Winter 2000): 127-143.

Ilachinski, Andrew. *Land Warfare and Complexity, Part I: Mathematical Background and Technical Sourcebook.* Alexandria, VA: Center for Naval Analyses, July 1996.

Kauffman, Stuart A. *At Home in the Universe.* New York: Oxford University Press, 1995.

Kenne, Leslie F. "Tightening the Noose: Separating the Control of Information from the Command, Control of Forces." *Intelligence, Surveillance, and Reconnaissance Journal* (January-February 2003): 10-15.

Levine, Alan J. *The War Against Rommel's Supply Lines, 1942-1943*. Westport, CT: Praeger Publishers, 1999.

Liebowitz, S. J. and Stephen E. Margolis. "Path Dependence, Lock-In, and History." *Journal of Law, Economics and Organization* (November 1995): 205-226.

Lupfer, Timothy L. *The Dynamics of Doctrine: The Changes in German Tactical Doctrine During the First World War*. Leavenworth Papers. Fort Leavenworth, KS: U.S. Army Command and General Staff College Combat Studies Institute, 1981.

McAfee, Andrew McAfee and François-Xavier Oliveau. "Confronting the Limits of Networks." *MIT Sloan Management Review* (Summer 2002): 85-87.

McCann, Carol and Ross Pigeau. *The Human in Command: Exploring the Modern Military Experience*. New York: Kluwer Academic/Plenum Publishers, 2000.

Metcalfe, Paul. "Metcalfe' Law: A Network Becomes More Valuable as it Reaches More Users." *Infoworld* (2 October 1995): 53.

Norretranders, Tor. *The User Illusion*. New York: Penguin Books, 1998.

Owens, William A. "An Emerging System of Systems." *U.S. Naval Institute Proceedings*, (May 1995): 35-39.

Pufeng, Wang. "The Challenge of Information Warfare." In *Chinese Views of Future Warfare*, edited by Michael Pillsbury, 317-326. Washington, DC: National Defense University Press, 1997.

Saperstein, Alvin M. "Complexity, Chaos, and National Security Policy: Metaphors or Tools?" In *Complexity, Global Politics, and National Security*, edited by David S. Alberts and Thomas J. Czerwinski, 101-134. Washington, DC: C4ISR Cooperative Research Program Publication Series, 1999.

Senge, Peter M. *The Fifth Discipline: The Art and Practice of the Learning Organization*. New York: Doubleday, 1990.

Shattuck, Lawrence. "Communicating Intent and Imparting Presence." *Military Review* (March-April 2000): 66-72.

Thomas, Timothy T. "Kosovo and the Current Myth of Information Superiority." *Parameters* (Spring 2000): 13-29.

Tse Tung, Mao. *On Guerrilla Warfare*. Trans. Samuel B. Griffith. University of Illinois Press, 1961.

Van Crevald, Martin. *Command in War*. New York: The Free Press, 1985.

_____. *Technology in War*. New York: The Free Press, 1991.

Vego, Milan N. *Operational Warfare*. Newport, RI: Naval War College Press, 1999.

Waldrop, Mitchell M. *Complexity: The Emerging Science at the Edge of Order and Chaos*. New York: Simon and Schuster, 1992.

Watts, Barry D. *Clausewitzian Friction and Future War*. McNair Paper 52. Washington, DC: National Defense University Press, 1996.

Windrum, Paul and G.M. Swann. *Networks, Noise, and Web Navigation: Sustaining Metcalfe's Law through Innovation*. MERIT Paper 009. Maastricht: Maastricht Economic Research Institute on Innovation and Technology, 1999.

Zimm, Alan D. "Human-Centric Warfare." *U.S. Naval Institute Proceedings* (May 1999): 28-31.